

AF\$
JW

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Rosenberg

Examiner: Vaughn

Serial No.: 09/559,414

Group Art Unit: 2131

Filed April 26, 2000

For: METHOD AND SYSTEM FOR SIGNING AND AUTHENTICATING
ELECTRONIC DOCUMENTS

BRIEF ON APPEAL

Commissioner of Patents and Trademarks
Arlington, Virginia 22313-1450

Sir:

Further to the Notice of Appeal filed January 14, 2005, herewith are three copies of Appellants' Brief on Appeal. The statutory fee of \$250 for the Notice of Appeal fee was paid on January 14, 2005. The \$250 fee for the submission of the appeal brief is enclosed herewith. Please charge any additional fee or credit any overpayment to Deposit Account No. 13-3403. Three copies of this page are attached for this purpose.

I. PRESENTATION OF THE APPEAL

A. Real Party in Interest

The real party in interest is Appellants' assignee, ProNvest, Inc., a Delaware corporation with its principal place of business at 375 Northridge Road, Suite 500, Atlanta, GA 30350.

B. Related Appeals and Interferences

There are no related appeals and interferences.

C. Status of Claims

At the time of the final Office Action, claims 1-45 were pending in the application. The application was initially filed with 45 claims. Some of the claims were amended with an Amendment and Response filed June 2, 2004 in response to the Office Action of December 3, 2003.

A copy of the claims subject to this appeal appears in Appendix A.

D. Status of Amendments

No proposed amendments have been proposed or entered after final.

E. Summary of Invention

Most generally, the present invention relates to a method and system for signing, storing, and authenticating electronic documents. (Page 1, lines 6-7). More specifically, the system and method include centrally maintaining a database containing at least portions of private encryption keys which are associated with users of the document and authenticating system. (Page 4, lines 10-12) The private encryption key portions can be used by the system together with non-public information received from users, for temporarily constructing or reconstructing complete private encryption keys that can be used for signing, encrypting, and decrypting. (Page 4, lines 12-15) Alternatively, if complete private keys are stored in the database, complete private encryption key constructing and reconstructing can be avoided. (Page 4, lines 17-18). The database can be made into a secured database requiring appropriate authorization from users. (Page 4, lines 18-20). A local computer cluster is useful to provide restricted access. (Page 5,

lines 4-6). The local cluster may be connected to remote computers via a network. (Page 5, lines 6- 7).

The first user (at a first remote computer), sends a signing request to the local computer cluster which is recognized by the local computer as being by the first user and identifying a signature ready document to be signed. (Page 5, lines 10-13). One way of communicating the signing request is to have the first user access a web site of the local computer cluster via the internet, transmit user identification, passwords, or other non-public information (i.e., signing identification credentials) to the local computer cluster using a browser with hypertext transport protocol (“HTTP”) to identify the document to be signed. (Page 5, lines 15-21).

A private key portion associated with the first user is then retrieved from the private key database for use in signing the signature ready document to be signed (which can be retrieved at the local computer cluster from the user computer, other computers, or the local computer cluster itself). (Page 6, lines 1-8). The signature ready document is then signed on the local computer cluster. (Page 6, line 3). Accordingly, the user computer **104** does not need to run dedicated software such as an add-in program, to enable a user to access and sign documents. (Page 8, lines 21-22)

In the preferred embodiment, the system and method allows users to view, modify and sign documents made available to them over the internet by a document owner. (Page 8, lines 17-18). A document owner or a user can prepare documents for signing by users. (Page 9, lines 1-2, and 4). Signature ready documents can be stored in a document safe **105**, the document owner server **103**, or the document service cluster **102** (i.e., a first document database). (Page 9, lines 2-4), (Claim 8). Signature ready

documents can be prepared in a standard generalized markup language (“SGML”). (Page 9, lines 6-7). Signing can be automatic by clicking a signing line. (Page 9, lines 12-13). Signature ready documents can be modified by retrieving a stored copy of a signature ready document and modifying with form data entered on a user computer 104. (Page 9, lines 17-22).

In a first method, a user signs a document by clicking on an icon displayed on a browser to cause a signing request to be transmitted from the user computer **104** to the document service provider via the web. (Page 10, lines 4-6). The signing request is received at the document service cluster **102** as shown in Figure 2. (Page 10, lines 6-7). In response to the signing request, the document service provider identifies the user and confirms the user is authorized to sign the document in an identification process. (Page 10, lines 7-9). The identification process includes engaging the user in a request-response interrogation. (Page 10, lines 9-10).

When the signature ready document is on the user computer 104 (such as downloaded from a website), the document server provider can download a copy of the signature ready document, together with any modifications from the user computer 104. (Page 10, lines 12-15). The user’s private key may be retrieved from a database maintained by the document service provider and appended to the document to provide a signed document. (Page 10, lines 20-22). The user’s handwritten signature can also be appended to the signed document to signify that the document has been digitally signed. (Page 10, line 23 – Page 11, line 2).

In addition to appending the handwritten signature of the user to the document, the document can be hashed **1007** as shown in Figure 10. (Page 32, line 18). The

protocol can locate and retrieve the user's private key **1008**, and encrypt the hash with the private key **1009**. (Page 32, lines 18-20). The encrypted hash can then be attached to the finally amended document **1010**. (Page 32, lines 20-21).

Alternatively, after the document service provider receives the signing request and signing identification credentials from the user, the document service provider may then construct a user private key by applying an algorithm to a private key portion retrieved from a database maintained by the document service provider and to the signing identification credentials (i.e., passwords, personal identification numbers, recognition graphics, biometric information) received from the user. (Page 11, lines 5-10). After signing the document, the constructed private key is destroyed thereby providing a security feature. (Page 11, lines 11-14). A user certificate can also be appended to a signed document. (Page 11, lines 16-17).

The document safe **105** storing signature ready documents may be connected to the document service cluster **102** via a dedicated connection or the internet. (Page 8, lines 3-10). Signed documents are stored in a user filing cabinet **215** which is a database maintained by the document service provider for each user. (Page 12, lines 3-6). Users and document owners can control access to the signed and signature ready documents can control access to the signed and signature ready documents located in their filing cabinets **215** or document safes **105**, such as on a secure second remote computer (Page 12, lines 14-15)(Claim 13).

The document service provider notifies the document owner and users when documents in the filing cabinets or document safes are accessed for signing or viewing.

(Page 13, lines 1-2). When a new signed document is created, all parties involved are notified that the signing is occurring. (Page 16, lines 6-7).

Users are preferably registered using a registration center **101** shown in Figure 1. (Page 19, lines 16-18). People wanting to register as users can present themselves at a registration center with identification documents. (Page 19, lines 16-18). At the registration center, a registration official can verify and witness the registration process. (Page 19, lines 18-21). The user can include recording and digitizing each user's signature, and recording biometric information such as, for example, finger prints, retina scans, and photographs. (Page 19, lines 21-24). Service credentials such as passwords, codes, graphics may also be provided at this time. (Page 20, lines 4-5). The recorded, digitized and service credentials may be grouped as identifying information and stored in a database. (Page 20, lines 10-11). A check may be made to detect people attempting to register under multiple identities. (Page 20, lines 13-14). The individual, after being authenticated, becomes a user and the user's registration information is provided to the document service cluster **102** from the registration computer. (Page 20, lines 20-22).

The local or document service cluster **102** comprises at least one computer. (Page 22, line 2). Figure 2 shows several computers connected to a network forming the document service cluster **102** including a database cluster **212**. (Page 22, lines 4-5, and 9). The database cluster **212** has an identity database **213**, a document database **213** and a filing cabinet within the identity database **213**. (Page 23, lines 1-3). A web cluster interfaces between remote client computers (users) via the firewall computer **202** and the core cluster **207**. (Page 23, lines 4-5) The core cluster **207** interfaces between the web cluster **203** and the database computer **212**. (Page 23, lines 5-6) A business tier **210**

comprised of core system programs run on the application server **208** within the core cluster **208**. (Page 23, line 21-22).

Insourced and outsourced configurations are envisioned for the signing and authentication system. (Page 25, lines 8-9, and 18). In an outsourced configuration, the signature ready and signed documents are maintained on databases in the document service cluster **102**. (Page 25, lines 9-11). In an insourced configuration, a document safe **105** may be provided to the document owner. (Page 25, lines 18-19). The document safe **105** has hardware and software for storing signature ready and signed documents and can be part of the document owner server **103**, or can be set up as a separate server connected to the document owner server as shown in Figure 4. (Page 25, lines 19-23). If no document safe is utilized for signature ready documents, they may be stored on the document owner's website with the signed documents still stored in the document safe. (Page 26, lines 2-3, and 19-20).

The information provided by the user during the registration process is useful for verifying user's that attempt to sign documents. User names and PIN pairs can be utilized to search the identity database **213** for a user. (Page 27, lines 12-13). Recognition graphics may be selected amongst, such as with a non-keyboard selecting device, such as, for example, a mouse or a touch-sensitive screen. (Page 27, lines 16-17). The user selects the appropriate graphic. (Page 27, line 18). Requiring the individual to select a recognized graphic in this way provides security feature that helps to secure the document service cluster and protect authorized users from hackers. (Page 27, lines 19-21). The protocol may then allow the user to select a pass phrase **508** and check whether

the entered pass phrase is correct **509**. (Page 28, lines 1-3). If correct, the individual is identified as the registered user thereby allowing further options. (Page 28, lines 10-12).

F. Issues

1. Whether the Examiner properly rejected claims 1-4, 8-16, 25-29, 31, 36-40, and 44 as being obvious over Vollert et al, U.S. Patent No. 5,208,858 (hereinafter “Vollert”) in view of Ganesan, U.S. Patent No. 5,535,276 (hereinafter “Ganesan”) in the Final Office Action.

2. Whether the Examiner properly rejected claims 5-7, 17-21, 23, 30, 32-35, 41-43 and 45 as being obvious over Vollert and Ganesan, in view of Smithies, U.S. Patent No. 5,544,255 (hereinafter “Smithies”) in the Final Office Action.

3. Whether the Examiner properly rejected 24 as being obvious over Vollert in view of Smithies in the Final Office Action.

4. Whether the Examiner properly rejected 22 as being obvious over Vollert, Ganesan, and Smithies, in view of Shin U.S. Patent No. 6,351,634 (hereinafter “Shin”) in the Final Office Action.

G. Claims

1. Claims 1-2 stand or fall together and they should be considered together. Claim 3 has additional grounds for allowance, and should be considered separately. Claim 4 has additional grounds for allowance, and should be considered separately. Claims 8, and 10-14 have additional grounds for allowance, but stand or fall together and should be considered together. Claim 9 has additional grounds for allowance, and should be considered separately. Claims 15 and 16 have additional grounds for allowance, but stand or fall together and should be considered together.

Claims 25, 28, 29 and 33 stand or fall together and they should be considered together. Claim 26 has additional grounds for allowance, and should be considered separately. Claim 27 has additional grounds for allowance, and should be considered separately. Claim 31 has additional grounds for allowance, and should be considered separately.

Claims 36 and 44 stand or fall together and should be considered together. Claims 37 and 38 have additional grounds for allowance, but stand or fall together and should be considered together. Claim 39 has additional grounds for allowance, and should be considered separately.

2. Claims 5-7 stand or fall together and they should be considered together. Claims 17, 20, and 23 stand or fall together and should be considered together. Claim 18 has additional grounds for allowance, and should be considered separately. Claim 19 has additional grounds for allowance, and should be considered separately. Claim 21 has additional grounds for allowance, and should be considered separately. Claim 30 has additional grounds for allowance, and should be considered separately. Claim 32 has additional grounds for allowance, and should be considered separately.

Claims 34 and 35 stand or fall together and should be considered together. Claim 41 has additional grounds for allowance, and should be considered separately. Claim 42 has additional grounds for allowance, and should be considered separately. Claim 43 has additional grounds for allowance, and should be considered separately. Claim 45 has additional grounds for allowance, and should be considered separately.

3. Claim 24 should be considered by itself.

4. Claim 22 should be considered by itself.

II. ARGUMENT

A. Obviousness Rejection of Claims 1-4, 8-16, 25-29, 31, 36-40, and 44

Based on Vollert in view of Ganesan

1. Rejection of Claims 1-2

The method of claim 1 essentially provides seven steps:

- (a) securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster;
- (b) receiving at the local computer cluster a signing request transmitted from a first remote computer in the absence of a pre-installed add in software program configured to providing a signed message at the remote computer;
- (c) identifying the signing request as one transmitted by the first user and identifying a signature ready document to be signed;
- (d) retrieving at the local computer cluster a private key portion associated with the first user from the private key database;
- (e) generating a complete private key if the retrieved private key portion is not a complete private key;
- (f) retrieving at the local computer cluster the signature ready document to be signed; and
- (g) signing the signature ready document at the local computer cluster with the generated private key.

The applicant does not agree with the characterization of the Examiner that Vollert discloses: “a method of signing and authenticating electronic documents comprising securely storing a plurality of private keys associated with a plurality of users

in a private key database on a local computer cluster.” (col. 3, lines 33-40). In this characterization, the private key database includes private key 9a stored at the central server 2 as shown in Figures 1 and 2 of Vollert. The “electronic documents” referred to by the Examiner appear to be the hash results 3 provided by the hash computer 16 which is shown as a portion of personal computer (PC) 15. As explained by Vollert, hash results 3 are not electronic documents:

“In that **it is not the entire document** that can also be very extensive that is sent to the receiver, an advantage of shorter transmission times occurs. Simultaneously, **it is not the document content that is sent to the server, but only a number**, the hash result, **from which the document cannot be reconstructed.**” (Vollert, Col. 2, lines 31-36)(emphasis added).

The applicant has utilized very similar terminology whereby the documents 1 in Vollert are the equivalent of “signature ready documents” utilized by the Applicant and the process of hashing is understood and described by the applicant (Page 18, lines 18-21) which is utilized independently of the signing of “signature ready documents” throughout the specification. It is important to recognize that the “signature ready document” or document 1 remains at the PC 15 and is NEVER sent to, or retrieved by, the central server 2 in Vollert. The step of retrieving the signature ready document to be signed at the local computer cluster (i.e., the central server 2) is not performed in Vollert.

The Applicant maintains that Vollert expressly teaches against sending the signature ready document to the central server: “Since the useful data are compressed to a defined length as a result of the hash event, a shorter transmission time results.” (Col. 3, lines 35-37). More importantly:

“In that **it is not the entire document** that can also be very extensive that is sent to the receiver, an advantage of shorter transmission times occurs. Simultaneously, **it is not the document content that is sent to the server, but**

only a number, the hash result, from which the document cannot be reconstructed.” (Vollert, Col. 2, lines 31-36)(emphasis added).

Accordingly Vollert teaches against sending the document to the local computer cluster and therefore utilizing Vollert as the teaching for the element of sending a document to a local computer cluster as a portion of an obviousness rejection is improper under the cases cited by MPEP § 2145 (See X. Arguing Improper Rationales for Combining References, D. References Teach Away from the Invention Render Prior Art Unsatisfactory for Intended Purpose) and MPEP § 2141.02, namely *In re Grasselli*, 713 F.2d 731, 743, 218 USPQ 769, 779 (Fed. Cir. 1983) and *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984).

Additionally, the Examiner does not address the transmission of a signing request from the local computer to the local computer cluster apart from citing almost the entire second column of Vollert. The hash result 3 is transmitted from the local computer 15 to the central server 2, and authentication of the user occurs (Vollert, Col. 2, lines 26-27), but the applicant has not located a signing request independent of the hash result or authentication of the user in the second column of Vollert as it relates to a signature ready document and not the hash result. In Vollert’s own words: “**Documents** infested with ‘viruses’ and the like **can therefore not proceed into the server process region at all.**” (Vollert, Col. 3, lines 6-8). The Applicant has been unable to locate this element in Vollert based on the rationale provided by the Examiner.

The Examiner correctly identifies that: “Vollert is silent in expressly disclosing storing private key portions and retrieving at the local computer cluster a private key portion associated with the first user from the private key database generating a complete

private key using the retrieved private key portion if the retrieved private key portion is not a complete private key.”

The Final Office Action, similar to the First Office Action, utilizes Ganesan for the proposition that a private key portion associated with the first user is retrieved from a private key database and utilized to generate a complete private key. Ganesan does not appear to teach the signing of documents “in the absence of a pre-installed add-in software program configured to provide a signed message at the remote computer.” Ganesan also does not appear to teach signing documents at the local computer cluster. In fact, a “temporary public key portion, is first generated, e.g. on a personal computer workstation or other processing device, by a first user” and then encrypted to form a first encrypted message. (Ganesan, col. 8, lines 22-27). This is not occurring at a local computer cluster.

Since neither Ganesan, nor Vollert, nor the combination, teach signing a document at the local computer cluster as claimed by the Applicant and explained above, claims 1 is believed to be allowable. Claims 2 and 8 depend from claim 1. Allowance of claims 1, 2 is respectfully requested.

2. Rejection of Claim 3

Claim 3 depends from claim 1 and requires the additional elements of receiving (a) signing identification credentials at the remote computer after receiving the signing request and (b) constructing a complete private key using the signing identification credentials. The Final Office Action cites Ganesan, column 12, lines 45-65 and column 14, lines 10-40 for these elements.

The Applicant has been unable to find support within the cited portions of Ganesan for these limitations. In column 12, lines 45-65, Ganesan discusses authentication from one user to another, but does not discuss using the signing credentials to construct a complete private key. In column 14, lines 10-40, Ganesan teaches the creation and issuance of an asymmetric crypto-key **before** a signing request is sent from to a local computer cluster, not **after**, as claimed in claim 3. (Ganesan, col. 14, lines 28-33).

Additionally, claim 3 depends from claim 1 and is believed to be allowable on those separate grounds as discussed above for claims 1 and 2. Allowance of claim 3 is respectfully requested.

3. Rejection of Claim 4

Claim 4 depends from claim 1 and requires the additional element of transmitting a signing request from the remote computer to the local computer cluster over the internet. The Applicant is confused by the Examiner's rejection of this claim. The Examiner states that Vollert teaches a system communicating over a network citing column 1, lines 54-56. Lines 54-58 of column 1 describe a disadvantage of communicating via "a line" as there is "the possibility of inadmissible manipulations." Nevertheless, the Examiner states that it would have been obvious to use the internet since it is "a huge network."

It appears that Vollert teaches against such use. Accordingly the basis of this separate rejection appears to be inaccurate. However, claim 4 depends from claim 1 and should be additionally allowable for the rationale described above for claim 1 as well as this basis.

4. Rejection of Claims 8, and 10-14

Claim 8 depends from claim 1 and requires the additional limitation of storing the signature ready document in a first database. The Examiner cites Vollert, col. 2, lines 40-44 for this element:

Due to the deposit of the signatures in the central server, the individual signing procedures of several users can be documented, so that an independent monitoring possibility is here available for legally binding promises in litigation.

It is the signatures that are retained “in the central server” in Vollert. There is no discussion of maintaining a database of signature ready documents. Furthermore, it is the hash results which are signed at the central server in Vollert are NOT signature ready documents. The document “**cannot be reconstructed**” from the hash result. (Vollert, col. 2, lines 35-36)(emphasis added). There does not appear to be a teaching for providing a database for the signature ready documents, or documents 1, in Vollert, certainly not where cited by the Final Office Action.

Accordingly, in addition to being allowable for the rationale provided above for claim 1, this separate argument provides another ground for allowance of claim 8. Claims 10-14 stand or fall with claim 8.

5. Rejection of Claim 9

Claim 9 depends from claim 8 and includes the additional limitations of receiving form data from the first remote computer and modifying the retrieved signature ready document based on the received form data. The Final Office Action cites col. 2, lines 10-11 for these additional elements:

“...signature with a crypto algorithm after the successful authentication of the user, in that this signature is...”

There is NOTHING in this cited passage which teaches or suggesting modifying a signature ready document with form data prior to signing the document with all of this occurring at the local computer cluster. There is not believed to be teaching in Vollert, Ganesan, or the combination, for this limitation.

Claim 9 is allowable for this separate rationale as well for the rationale provided above for claims 1 and 8 from which claim 9 depends.

6. Rejection of Claims 15 and 16

Claim 15 depends from claim 12 (which depends from claim 8) and requires the additional limitation of associating at least one of the signature ready documents and the signed document with a document owner. The Final Office Action cites Vollert, col. 2, lines 10-13 for this limitation:

“...signature with a crypto algorithm after the successful authentication of the user, in that this signature is deposited in the central server and is transmitted simultaneously to the user for checking, together with the...”

It is important to remember that the signature ready documents (documents 1) are never sent to the central server (local computer cluster), and are never associated with a signed document in Vollert. The particular citation relied upon by the Final Office Action does not make sense.

Accordingly, claim 15 is allowable on this separate rationale as well as that provided above for claims 1 and 8, from which claims 15 depends (indirectly from claim 12, which stands or falls with claim 8). Claim 16 depends from claim 15 and stands or falls with claim 16.

7. Rejection of Claim 25, 28, 29 and 33

Claim 25 is an independent claim somewhat similar to claim 1, but requires a generating a complete private key at the local computer cluster independent of a private key portion provided from the first remote computer. Ganesan requires a private key portion to be provided from the remote computer. (Ganesan, Col. 8, lines 19-28). Vollert provides a private key at a local computer cluster, but does not use it to sign documents, only to sign hash results as explained above as it relates to claim 1. Accordingly neither Ganesan, nor Vollert, nor the combination teach this element of claim 25.

Furthermore neither Ganesan, nor Vollert, nor then combination, teach the elements of (1) retrieving a signature ready document at the local computer cluster, or (2) signing a signature ready document at the local computer cluster, as discussed in detail above as it relates to claims 1 and 2. Ganesan does not appear to mention any capability of signing a document at the local computer cluster and Vollert expressly teaches away from it: “...[I]t is **not the document content that is sent to the server, but only a number, the hash result, from which the document cannot be reconstructed.**” (Vollert, Col. 2, lines 34-36)(emphasis added).

Accordingly, for at least these two reasons, claim 25 is believed to be allowable, and such action is respectfully requested. Claims 28, 29, and 33 depend from claim 25 and stand or fall with claim 25.

8. Rejection of Claim 26

Claim 26 depends from claim 25 and requires the additional limitation of storing the signature ready document in a database remote from the local computer cluster in a

second remote memory device to the limitations of those found in claim 25. The

Examiner cites Vollert, col. 2, lines 40-44 for this element:

Due to the deposit of the signatures in the central server, the individual signing procedures of several users can be documented, so that an independent monitoring possibility is here available for legally binding promises in litigation.

It is the signatures that are retained “in the central server”, there is no discussion of maintaining a database of signature ready documents. Furthermore, it is the hash results which are signed at the central server in Vollert are NOT signature ready documents. The document “cannot be reconstructed” from the hash result. (Vollert, col. 2, lines 35-36). There is no teaching for providing a database for the signature ready documents, or documents 1, in Vollert.

Accordingly, in addition to being allowable for the rationale provided above for claim 25, this separate argument provides another ground for allowance of claim 26.

9. Rejection of Claim 27

Claim 27 depends from claim 25 and requires the additional limitation of storing the signature ready document in a database in a memory device coupled to the processor to the limitations found in claim 25. The Examiner cites Vollert, col. 3, line 17 for this element:

“...ized in that the deposit of the signature in the central server occurs by at least doubling the deposit memory...”

It is the signatures that are retained “in the central server”, there is no discussion of maintaining a database of signature ready documents. Furthermore, it is the hash results which are signed at the central server in Vollert are NOT signature ready documents. The document “cannot be reconstructed” from the hash result. (Vollert, col. 2, lines 35-

36). There is no teaching for providing a database for the signature ready documents, or documents 1, in Vollert.

Accordingly, in addition to being allowable for the rationale provided above for claim 25, this separate argument provides another ground for allowance of claim 27.

10. Rejection of Claim 31

Claim 31 depends from claim 25 and includes the additional limitations of receiving form data from the first remote computer and modifying the retrieved signature ready document based on the received form data, wherein the form data is received independent of at least one of signing identification credentials and public and private key information. The Final Office Action cites col. 2, lines 10-11 for these additional elements:

“signature with a crypto algorithm after the successful authentication of the user, in that this signature is”

There is NOTHING in this cited passage which teaches or suggesting modifying a signature ready document with form data prior to signing the document with all of this occurring at the local computer cluster. There is not believed to be teaching in Vollert, Ganesan, or the combination, for this limitation.

Claim 31 is allowable for this separate rationale as well for the rationale provided above for claim 25 from which claim 31 depends.

11. Rejection of Claim 36 and 44

Claim 36 is another independent claim that requires “means for retrieving the at the local computer cluster the signature ready document to be signed” and “a means for signing the signature ready document at the local computer cluster...”. As discussed above for independent claims 1 and 25, these two elements are not present in Vollert and

the signing of a document is expressly taught away from by Vollert: “...[I]t is not the document content that is sent to the server, but only a number.” (Vollert, Col. 2, lines 34-35). These two elements are similarly not found in Ganesan.

In this claim, generation of the private key occurs independent of receiving a public and private key portion from the first user. As explained above for claim 25, Ganesan teaches at least the provision of a private key portion from the first user (Ganesan, Col. 8, lines 19-24). Vollert teaches signing a hash result 3 (i.e., a number, not a document).

Accordingly an improper obviousness rejection has been formulated. Claim 36 is believed to be allowable, and such action is respectfully requested. Claim 44 depends from claim 36 and stands or falls with claim 36.

12. Rejection of Claims 37 and 38

Claim 37 depends from claim 36 and requires the additional limitation of storing the signature ready document in a first document database. The Examiner cites Vollert, col. 2, lines 40-44 for this element:

Due to the deposit of the signatures in the central server, the individual signing procedures of several users can be documented, so that an independent monitoring possibility is here available for legally binding promises in litigation.

It is the signatures that are retained “in the central server”, there is no discussion of maintaining a database of signature ready documents. Furthermore, it is the hash results which are signed at the central server in Vollert are NOT signature ready documents. The document “cannot be reconstructed” from the hash result. (Vollert, col. 2, lines 35-36). There is no teaching for providing a database for the signature ready documents, or documents 1, in Vollert.

Accordingly, in addition to being allowable for the rationale provided above for claim 36, this separate argument provides another ground for allowance of claim 37. Claim 38 depends directly from claim 37 and stands or falls with claim 37.

13. Rejection of Claim 39

Claim 39 depends from claim 38 and requires the additional limitation of associating at least one of the signature ready documents and the signed document with a document owner. The Final Office Action cites Vollert, col. 2, lines 10-13 for this limitation:

“signature with a crypto algorithm after the successful authentication of the user, in that this signature is deposited in the central server and is transmitted simultaneously to the user for checking, together with the”

It is important to remember that the signature ready documents (documents 1) are never sent to the central server (local computer cluster), and are never associated with a signed document. The particular citation relied upon by the Final Office Action is nonsensical.

Accordingly, claim 39 is allowable on this separate rationale as well as that provided above for claims 36 and 37, from which claims 39 depends (indirectly from claim 38, which stands or falls with claim 37). Claim 40 depends from claim 39 and stands or falls with claim 39.

B. Obviousness Rejection of Claims 5-7, 17-24, 30, 32-35, 41-43, and 45 Based on Vollert and Ganesan in view of Smithies

1. Rejection of Claims 5-7

Claim 5 depends from claim 1 and requires the additional limitation of transmitting the signing request over the world wide web using hypertext transport protocol using a browser running on the remote computer. The Final Office Action

acknowledges that Vollert is silent as to teaching the use of a web browser and hypertext markup languages to send a signing request. For this limitation the Office Action states:

Smithies teach a commerce system that utilizes the WWW to securely transmit documents with Web browsers using HTML (see col. 41, line 64-col. 43, line 10). (emphasis added)

First, Smithies ends at column 34. There are no columns 41, 42 and 43. Second, in column 2, Smithies states:

It is noted that the term ‘signature’ as used herein does not include what has come to be known in computer science fields as a ‘digital signature’, i.e., an electronic code that is used to establish the identity of the person creating or sending electronic documents. A ‘digital signature’ has the function of replacing a handwritten signature, with a secret alphanumeric ‘key’ supplied to a given individual which then has to be kept secret. In contrast, the present invention is directed to electronically capturing and manipulating a person’s handwritten signature. (Smithies, Col. 3, lines 48-58).

The applicant is unable to find any reference in Smithies for the additional limitation added by claim 5. Furthermore, even if the element is present, Smithies relates to an individual’s handwritten signature (i.e., “autograph”). There is no teaching or suggestion to combine Smithies with digital signatures, especially when Smithies states: “It is noted that **the term ‘signature’ as used herein does not include what has come to be known in computer science fields as a ‘digital signature’....**” (Col.3, lines 48-51).

Accordingly, this reference also teaches against the claimed combination provided by claim 5. Furthermore, there is no motivation to combine Smithies with either Ganesan or Vollert.

There is no teaching or suggestion by Vollert, Ganesan and/or Smithies for the additional limitation of transmitting the signing request over the world wide web using hypertext transport protocol using a browser running on the remote computer. Claim 5 depends directly from claim 1 and is believed to be allowable for the rationale provided

above for claim 1. Additionally, claims 6 and 7 depend directly from claim 5. Claims 6 and 7 stand or fall with claim 5. Allowance of claims 5-7 is respectfully requested.

2. Rejection of Claims 17, 20 and 23

Claims 17 depends from claim 1 and provides the additional limitations of verifying and recording the identity of individuals registering including biometric measurements, specifically (a) verifying and recording the identity of individuals registering, (b) digitizing and recording handwritten signatures of individuals registering, (c) associating passwords with the digitized handwritten signatures and the recorded identities, and (d) storing the recorded digitized handwritten signatures, and the recorded identities in an identity database accessible to the local computer cluster . The Final Office Action relies on col. 2, lines 9-10 and 66-68, and col. 3, lines 12-13 for a basis of rejection of these additional limitations.

The Examiner does not acknowledge that Smithies is directed to “digitized handwritten signatures” and not “digital signatures” (Smithies, Col. 3, lines 48-51). The fact that digitized handwritten signatures are stored in a database in Smithies does not meet the claimed limitations of claim 17.

Claim 17 depends from claim 1 and is allowable as explained above for the rationale provided for claim 1. Claim 20 depends directly from claim 17 and stands or falls with claim 17. Claim 23 depends directly from claim 17 and stands or falls with claim 17. Allowance of claims 17, 20 and 23 is respectfully requested.

3. Rejection of Claim 18

Claim 18 depends from claim 17 was rejected along with claim 17 for the identical reasoning. Claim 18 was amended in June 2004 to require at least one biometric measurement other than a handwritten signature to be stored in the identity database.

The applicant has been unable to find this limitation in the cited references and therefore maintains that a prima facie case of obviousness has not been met. Allowance of claim 18 on this separate basis is also requested.

4. Rejection of Claim 19

Claim 19 depends from claim 18 and requires detecting using the biometric measurements to ascertain whether individuals have previously registered. The Final Office Action states: "Vollert teaches the biometric measurements can determine whether individuals have previously registered. This is an obvious conclusion to using biometric identification to identify a user as taught in col. 3., lines 12-14."

Col. 3, lines 12-14 of Vollert states that biometric methods can be employed for user authentication:

"The effectiveness of the user authentication can be increased, according to the present invention, in that biometric methods are employed."

Nothing in this citation teaches or suggests utilizing biometric information to determine if individuals have previously registered, only for authenticating a particular user. It appears to be entirely possible for one individual in Vollert to have a plurality of identities which are "users" in the Vollert system. It is only using the Applicant's disclosure, and NOT the cited reference, that the rationale is located for rejecting this claim. This is believed to be an improper obviousness rejection.

Claim 19 depends from claim 18 and is separately allowable for the rationale for claim 18 and the claims from which claim 18 depends. Allowance is respectfully requested.

5. Rejection of Claim 21

Claim 21 depends from claim 20 and requires the additional limitations of (a) appending the first user's digitized handwritten signature to the signature ready document, (b) making a hash of the signature ready document, and (c) encrypting the hash with the user's private key. The Examiner relies on Smithies, col. 20, lines 23-64 and col 13, lines 36-56 to make the rejection.

Smithies col. 20, lines 23-64 relate to a method of verifying that a document alleged to be signed is the same document which is signed (with a handwritten signature) by performing a checksum (a mathematical algorithm) on the ASCII characters to tell if the document has been changed. Col. 13, lines 36-56 relates to the digitizing of an image of a handwritten signature and then performing a checksum on the digitized data along with data such as date and time of signing, the machine used to perform the handwritten signature, etc....

There does not appear to be any teaching in ANY of the cited references for (a) appending the first user's digitized handwritten signature to the signature ready document, (b) making a hash of the signature ready document, and (c) encrypting the hash with the user's private key. There is teaching in Vollert for making a hash of a signature ready document and encrypting the has with the user's private key, but there is no teaching in any references for appending a digitized handwritten signature to the

signature ready document prior to making the hash. Accordingly allowance of claim 21 is respectfully requested.

Claim 21 depends from claim 17 and is separately allowable for the rationale for claim 17 and the claims from which claim 17 depends. Allowance is respectfully requested.

6. Rejection of Claim 30

Claim 30 depends from claim 25 and requires a second memory device having an identity database including handwritten signatures, recorded user identities associated with the signatures and passwords associated with the user identities. The Final Office Action states that Vollert teaches a second memory device having stored thereon an identity database citing column 3, lines 15-25. Column 3, lines 15-25 are provided below:

According to another advantageous development and feature of the invention, the method is characterized in that the deposit of the signature in the central server occurs by at least doubling the deposit memory in separate structures. A certain protection of the deposited data against minor catastrophes is thereby established. A further advantage development is that the invention is characterized in that, due to the doubling of the signature deposit, the deposit can be administered on a long-term basis and mutually monitorable by different cooperative entities.

There is nothing in this cited passage which provides the new claim limitations of claim 30. The cited references do not appear to provide a teaching or suggestion as to how the claimed combination could be performed. This is believed to be another improper obviousness rejection.

Additionally, claim 30 depends from claim 25 which is believed to be allowable as discussed above. Allowance is respectfully requested.

7. Rejection of Claim 32

Claim 32 depends from claim 25 and requires the additional limitations that the signature ready document have the signing request and activation of the signing request at the remote computer transmits the signing request to the local computer cluster. The Final Office Action states that “Vollert is silent as to teaching the use of a web browser and hypertext markup languages to send a signing request.” For this limitation the Office Action states:

Smithies teach a commerce system that utilizes the WWW to securely transmit documents with Web browsers using HTML (see col. 41, line 64-col. 43, line 10). (emphasis added)

First, Smithies ends at column 34. There are no columns 41, 42 and 43. Second, in column 2, Smithies states:

It is noted that the term ‘signature’ as used herein does not include what has come to be known in computer science fields as a ‘digital signature’, i.e., an electronic code that is used to establish the identity of the person creating or sending electronic documents. A ‘digital signature’ has the function of replacing a handwritten signature, with a secret alphanumeric ‘key’ supplied to a given individual which then has to be kept secret. In contrast, the present invention is directed to electronically capturing and manipulating a person’s handwritten signature. (Smithies, Col. 3, lines 48-58).

The applicant is unable to find any reference in Smithies for the additional limitation added by claim 32. Furthermore, even if the element is present, Smithies relates to an individual’s handwritten signature (i.e., “autograph”). There is no teaching or suggestion to combine Smithies with digital signatures, especially when Smithies states: “It is noted that **the term ‘signature’ as used herein does not include what has come to be known in computer science fields as a ‘digital signature’**” (Col.3, lines 48-51)(emphasis added). Accordingly, this reference also teaches against the claimed combination provided by claim 32. Furthermore, apparently the Examiner did not notice that claim 32

had been amended as it is unclear as to why reasoning with browsers and HTML language supports a rejection for the limitations the signature ready document have the signing request and activation of the signing request at the remote computer transmits the signing request to the local computer cluster.

There is no teaching or suggestion by Vollert, Ganesan and/or Smithies for the limitation of the signature ready document having the signing request and activation of the signing request at the remote computer transmitting the signing request to the local computer cluster. Claim 32 depends directly from claim 25 and is believed to be allowable for the rationale provided above for claim 25. Allowance of claims 25 is respectfully requested.

8. Rejection of Claims 34 and 35

Claim 34 depends from claim 25 and requires the additional limitation of a registration computer connected to the local computer cluster. The Final Office Action cites Vollert, col. 2, lines 66-68 for this limitation:

...the user authentication occurs with a satellite computer lying in the transmission path preceding the crypto algorithm computer in combination with the...

An authentication computer is the computer which checks to see if the user is, in fact, the registered user. There is no teaching or suggestion in the cited portion of Vollert that the authentication computer is capable of performing registration of individuals. This limitation does not appear to be met by the cited references.

Nevertheless, claim 34 depends from claim 25 and is believed to be allowable for the rationale provided above as it relates to that claim. Claim 35 depends directly from claim 34. Allowance of claims 34 and 35 is respectfully requested.

9. Rejection of Claims 41

Claims 41 depends from claim 36 and provides the additional limitations of verifying and recording the identity of individuals registering including biometric measurements, specifically (a) a means for verifying and recording the identity of individuals registering, (b) a means for digitizing and recording handwritten signatures of individuals registering, (c) a means for associating passwords with the digitized handwritten signatures and the recorded identities, and (d) a means for storing the recorded digitized handwritten signatures, and the recorded identities in an identity database accessible to the local computer cluster . The Final Office Action relies on col. 2, lines 9-10 and 66-68, and col. 3, lines 12-13 for a basis of rejection of these additional limitations.

Since the Examiner does not acknowledge that Smithies is directed to “digitized handwritten signatures” and not “digital signatures” (Col. 3, lines 48-51), the fact that digitized handwritten signatures are stored in a database in Smithies does not meet the claimed limitations of claim 41. Smithies does not appear to teach digital signatures.

Claim 41 depends from claim 36 and is allowable as explained above for the rationale provided for claim 36. Allowance is respectfully requested.

10. Rejection of Claim 42

Claim 42 was rejected along with claim 41 for the identical reasoning even though this claim as amended in June 2004 requires a means for recording at least one biometric measurement other than a handwritten signature stored in the identity database.

The applicant has been unable to find this limitation in any of the cited references and therefore maintains that a prima facie case of obviousness has not been met.

Allowance of claim 42 on this separate basis is also requested. Additionally, claim 42 depends from claim 41 and is believed to be allowable for the rationale above as it relates to claim 41.

11. Rejection of Claim 43

Claim 43 depends from claim 42 and requires using the biometric measurements to determine whether individuals have previously registered. The Final Office Action states: “Vollert teaches the biometric measurements can determine whether individuals have previously registered. This is an obvious conclusion to using biometric identification to identify a user as taught in col. 3., lines 12-14.”

Col. 3, lines 12-14 of Vollert states that biometric methods can be employed for user authentication:

“The effectiveness of the user authentication can be increased, according to the present invention, in that biometric methods are employed.”

Nothing in this citation teaches or suggests utilizing biometric information to determine if individuals have previously registered. It appears to be entirely possible for one individual in Vollert to have a plurality of identities which are “users” in the Vollert system. It is only using the Applicant’s disclosure, and NOT the cited reference, that the rationale is located for rejecting this claim. This is believed to be an improper obviousness rejection.

Claim 43 depends from claim 42 and is separately allowable for the rationale for claim 42 and the claims from which claim 42 depends. Allowance is respectfully requested.

12. Rejection of Claim 45

Claim 45 depends from claim 44 and requires the additional limitations of (a) a means for appending the first user's digitized handwritten signature to the signature ready document, (b) a means for making a hash of the signature ready document, and (c) a means for encrypting the hash with the user's private key. The Examiner relies on Smithies, col. 20, lines 23-64 and col 13, lines 36-56 to make the rejection.

Smithies col. 20, lines 23-64 relate to a method of verifying that a document alleged to be signed is the same document which is signed (with a handwritten signature) by performing a checksum (a mathematical algorithm) on the ASCII characters to tell if the document has been changed. Col. 13, lines 36-56 relates to the digitizing of an image of a handwritten signature and then performing a checksum on the digitized data along with data such as date and time of signing, the machine used to perform the handwritten signature, etc....

There does not appear to be any teaching in ANY of the cited references for (a) a means for appending the first user's digitized handwritten signature to the signature ready document, (b) a means for making a hash of the signature ready document, and (c) a means for encrypting the hash with the user's private key. There is teaching in Vollert for making a hash of a signature ready document and encrypting the has with the user's private key, but there is no teaching in any references for appending a digitized handwritten signature to the signature ready document prior to making the hash. Accordingly allowance of claim 45 is respectfully requested.

Claim 45 depends from claim 44 and is separately allowable for the rationale for claim 44 and the claims from which claim 44 depends. Allowance is respectfully requested.

C. Obviousness Rejection of Claim 24 Based on Vollert in view of Smithies

Claim 24 is an independent claim that requires running a browser on a first remote computer connected to a local computer cluster via a computer network, transmitting user identification information and document identification information to the local computer cluster, and transmitting a signing request to the local computer cluster from the remote computer independent of both a private key portion and a public key portion, the signing request requesting the local computer cluster to retrieve the identified document from a second remote computer, to obtain a private encryption key associated with the identified user from a third remote computer, and to sign the retrieved document using the obtained private key on a fourth computer, wherein the first, second, third, and fourth remote computers can be the same computer or different computers.

The Final Office Action mischaracterizes the teaching of Vollert to equate the hash result 3 to a document 1 (as identified in that reference). The central server 2 (local computer cluster) never “retrieves” an identified document from any computer. It receives the hash result from the PC 15 and signs the hash result. In fact, Vollert teaches away from signing documents:

“In that **it is not the entire document** that can also be very extensive that is sent to the receiver, an advantage of shorter transmission times occurs. Simultaneously, **it is not the document content that is sent to the server**, but only a number, the hash result, from which the document cannot be reconstructed.” (Vollert, Col. 2, lines 31-36)(emphasis added).

In Vollert's own words: "**Documents** infested with 'viruses' and the like **can therefore not proceed into the server process region at all.**" (Vollert, Col. 3, lines 6-8)(emphasis added). Smithies relates to digitized handwritten signatures, and similarly lacks at least this limitation.

Accordingly, claim 24 is believed to be allowable and allowance is respectfully requested.

D. Obviousness Rejection of Claim 22 Based on Vollert, Ganesan, and Smithies in view of Shin

Claim 22 depends from claim 17 and requires the additional limitation of the display of recognition graphics on the first remote computer selected from a secret set, the selection with a non-keyboard selecting device of a graphic, sending a message related to the selection, and authorizing access if a correct selection is performed in addition to the limitations provided for claim 17.

Shin teaches the use of the selection of a secret symbol amongst recognition graphics for use in accessing a digital mobile telephone instead of providing a password: "to guard against an authorized user from being unable to use the telephone due to forgetting the password or keying-in the wrong password." (Col. 2, lines 14-16). The purpose of the applicant is different: "Requiring the individual to select a recognized graphic in this way provides a security feature that helps to secure the document service cluster and protect authorized users from hackers." (Specification, Page 27, lines 19-21).

Furthermore, the applicant is having trouble taking the four references cited by the Final Office Action and formulating an obviousness rejection without using the Applicant's claim as the teaching or suggestion to make the claimed combination. Under

MPEP § 2145 (Section C. Lack of Suggestion to Combine), there is not believed to be a suggestion to combine the references existing in the prior art. Accordingly, the obviousness rejection is believed to be improper on this basis as well.

Nevertheless, since claim 22 depends from claim 17, the rationale provided above as it relates to claim 17 provides additional grounds for allowance of claim 22.

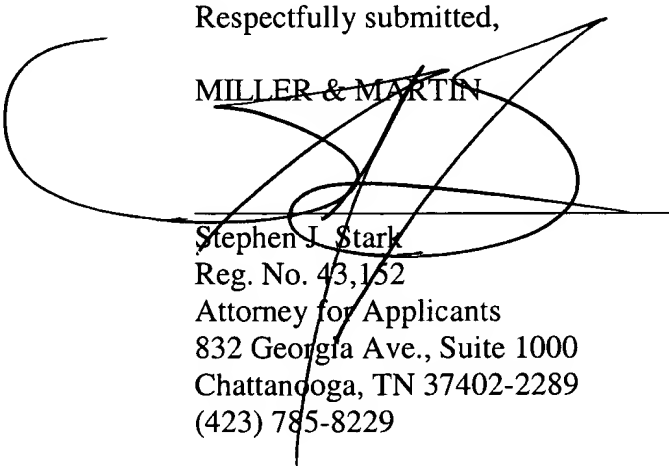
Allowance of claim 22 is respectfully requested.

III. CONCLUSION

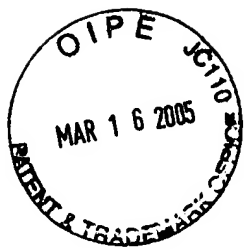
Claims 1-4, 8-16, 25-29, 31, 36-40, and 44 are not believed to be obvious over Vollert et al, U.S. Patent No. 5,208,858 (hereinafter "Vollert") in view of Ganesan, U.S. Patent No. 5,535,276 (hereinafter "Ganesan"), and claims 5-7, 17-21, 23, 30, 32-35, 41-43 and 45 are not believed to be obvious over Vollert and Ganesan, in view of Smithies, U.S. Patent No. 5,544,255. Claim 24 is not believed to be obvious over Vollert in view of Smithies. Finally Claim 22 is not believed to be obvious over Vollert, Ganesan and Smithies in view of Shin. Allowance of claims 1-45 is respectfully requested.

Respectfully submitted,

MILLER & MARTIN



Stephen J. Stark
Reg. No. 43,152
Attorney for Applicants
832 Georgia Ave., Suite 1000
Chattanooga, TN 37402-2289
(423) 785-8229



CERTIFICATE OF MAILING

I hereby certify that the preceding Brief on Appeal is being deposited with the United States Postal Service as first class mail in an envelope addressed to:

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, Virginia 22313-1450

On this 14th day of March, 2005.

Beverly L. Middleton
Beverly L. Middleton

APPENDIX A

1. (Amended 6/2/2004) A method of signing and authenticating electronic documents comprising:

securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster;

receiving at the local computer cluster a signing request transmitted from a first remote computer by a first user said signing request generated in the absence of a pre-installed add-in software program configured to providing a signed message at the remote computer;

identifying the signing request as one transmitted by the first user, and identifying a signature ready document to be signed;

retrieving at the local computer cluster a private key portion associated with the first user from the private key database;

generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key;

retrieving at the local computer cluster the signature ready document to be signed;
and

signing the signature ready document [on] at the local computer cluster using the generated complete private key to produce a signed document.

2. (Original) The method of claim 1 wherein the private key portion is a complete private key.

3. (Amended 6/2/2004) The method of claim 1 wherein generating a complete private key using the retrieved private key portion includes:

receiving signing identification credentials sent from the first user at the remote computer to the local computer cluster after receiving the signing request; and

constructing a complete private key using the private key portion and the received signing identification credentials.

4. (Original) The method of claim 1 wherein the received signing request was transmitted from the first remote computer to the local computer cluster over the internet.

5. (Original) The method of claim 1 wherein the received signing request was transmitted from the first remote computer to the local computer cluster over the world wide web using hypertext transport protocol, and wherein the signing request was transmitted using a browser running on the remote computer.

6. (Original) The method of claim 5 wherein the retrieving at the local computer cluster the signature ready document is automatic.

7. (Original) The method of claim 5 wherein the retrieved signature ready document is a standard generalized markup language document.

8. (Original) The method of claim 1 further comprising storing the signature ready document in a first document database.

9. (Original) The method of claim 8 further comprising prior to signing:

receiving form data from the first remote computer; and

modifying the retrieved signature ready document based on the received form date.

10. (Original) The method of claim 8 wherein the first document database is located on the local cluster.
11. (Original) The method of claim 8 wherein the first document database is located on a secure second remote computer.
12. (Original) The method of claim 8 further comprising storing the signed document in a second document database.
13. (Original) The method of claim 12 wherein the second database is located on a secure second computer remote computer.
14. (Original) The method of claim 12 wherein the second database is located on the local computer cluster.
15. (Original) The method of claim 12 further comprising associating at least one of the signature ready documents and the signed document with a document owner.
16. (Original) The method of claim 15 further comprising notifying at least one of document owner and the first user that a signature ready document or a signed document has been signed.
17. (Original) The method of claim 1 further comprising registering individuals as users, wherein registering includes:

verifying and recoding the identify of individuals registering;

digitizing and recording handwritten signatures of individuals registering;

associating passwords with the recorded digitized handwritten signatures and the recorded identities; and

storing the recorded digitized handwritten signatures, and the recorded identities in an identify database, the identify database being accessible to the local computer cluster.

18. (Amended 6/2/2004) The method of claim 17 further comprising:

recording at least one biometric measurement[s] other than a handwritten signature of individuals registering;

associating the at least one biometric measurement[s] of individuals registering with the recorded identities of the individuals registering; and

storing the biometric measurements in the identity database.

19. (Original) The method of claim 18 further comprising detecting using the biometric measurements whether individuals previously registered.

20. (Original) The method of claim 17 wherein the first user is a registered owner.

21. (Amended 6/2/2004) The method of claim 20 wherein the signing comprises:

a) appending the first user's digitized handwritten signature to the signature ready document;

b) making a hash of the signature ready document; and

c) encrypting the hash of the signature ready document with the first user's private key.

22. (Original) The method of claim 17 further comprising:

associating and storing a secret set of recognition graphics with the passwords in the identity database;

displaying a plurality of recognition graphics, including recognition graphics from the secret set, on the first remote computer;

requesting the first user to select graphics including in the secret set using a non-keyboard selecting device attached to the first remote computer;

receiving a message from the first remote computer identifying the selected graphics;

authorizing access to the local computer cluster if the selected graphics are included in the secret set.

23. (Original) The method of claim 17 further comprising:

generating the private key portions for individuals registering, wherein the private key portions can be used with signing identification credentials to construct complete private keys;

associating the generated private key portions with the recorded identities of individuals registering; and

storing private key portions in a private key database.

24. (Amended 6/2/2004) A method of signing and authenticating electronic documents comprising:

running a browser on a first remote computer;

connecting to a local computer cluster via a computer network using the browser;

transmitting user identification information and document identification information to the local computer cluster; and

transmitting a signing request to the local computer cluster from the remote computer independent of both a private key portion and a public key portion, the signing request requesting the local computer cluster to retrieve the identified document from a second remote computer, to obtain a private encryption key associated with the identified user from a third remote computer, and to sign the retrieved document using the obtained private key on a fourth computer, wherein the first, second, third, and fourth remote computers can be the same computer or different computers.

25. (Amended 6/2/2004) A system for signing and authenticating documents comprising local computer cluster, the local computer cluster including:

a first memory device having a first program store thereon; and

a first processor coupled to the first memory, wherein the first processor can read the first program stored in the first memory and can perform the steps of:

securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster;

receiving at the local computer cluster a signing request transmitted from a first remote computer by a first user;

identifying the signing request as one transmitted by the first user, and identifying a signature ready document to be signed;

retrieving at the local computer cluster a private key portion associated with the first user from the private key database.

generating at the local computer cluster independent of a private key provided from the first remote computer a complete key using the retrieved private key portion of the retrieved private key portion is not a complete private key;

retrieving at the local computer cluster the signature ready document to be signed;
and

signing the signature ready document [on] at the local computer cluster using the generated complete private key to produce a signed document.

26. (Original) The system of claim 25 further comprising a second remote memory device having stored thereon a signature ready document database, wherein the second memory device is remotely connected to the local computer cluster.

27. (Original) The system of claim 25 wherein the local computer cluster further comprises a second memory device having stored thereon a signature ready document database, wherein the second memory device is coupled to the processor.

28. (Original) The system of claim 25 further comprising a second memory device having stored thereon a signed document database, wherein the second memory device is remotely connected to the local computer cluster.

29. (Amended 6/2/2004) The system of claim 25 wherein the local computer cluster further comprises a second memory device having stored thereon a signed document database, wherein the [third] second memory device is coupled to the processor.

30. (Original) The system of claim 25 wherein the local computer cluster further comprises a second memory device having stored thereon an identity database, the identity database including user digitized handwritten signatures, recorded user identities associated with the signatures, and passwords associated with the user identifies.

31. (Amended 6/2/2004) The system of claim 25 wherein the processor can perform the additional steps of:

receiving form data independent of at least one of signing identification credentials, and public and private key information from the first remote computer; and

modifying the retrieved signature ready document based on the received form data.

32. (Amended 6/2/2004) The system of claim 25 wherein the received signature ready document [is a standard generalized markup language document] further comprises the signing request, and activation of the signing request at the remote computer transmits the signing request to the local computer cluster.

33. (Original) The system of claim 25 wherein the retrieving at the local computer cluster the signature ready document is automatic.

34. (Original) The system of claim 25 further comprising a registration computer connected to the local computer cluster.

35. (Original) The system of claim 34 wherein the registration computer comprises a second memory device having a second program stored thereon; and

a second processor coupled to the second memory, wherein the second processor can read the second program stored in the second memory and can perform the steps of:

recording the identify of individuals registering;

and recording digitized handwritten signatures of individuals registering;

associating passwords with the recorded digitized handwritten signatures and the recorded identities; and

storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identify database being accessible to the local computer cluster.

36. (Amended 6/2/2004) A system for signing and authenticating documents comprising:

a means for securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster;

a means for receiving at the local computer cluster a signing request transmitted from a first remote computer by a first user;

a means for identifying the signing request as one transmitted by the first user, and identifying a signature ready document to be signed;

a means for retrieving at the local computer cluster a private key portion associated with the first user from the private key database independent of receiving both a public and a private key portion from the first user;

a means for generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key at the local computer cluster;

a means for retrieving at the local computer cluster the signature ready document to be signed; and

a means for signing the signature ready document [on] at the local computer cluster using the generated complete private key to produce a signed document.

37. (Original) The system of claim 36 further comprising a means for storing the signature ready document in a first document database.

38. (Original) The system of claim 37 further comprising a means for storing the signed document in a second document database.
39. (Original) The system of claim 38 further comprising a means for associating at least one of the signature ready document and the signed document with a document owner.
40. (Original) The system of claim 39 further comprising a means for notifying at least one of document owner and the first user that a signature ready document or a signed document has been signed.
41. (Original) The system of claim 36 further comprising a means for registering individuals as users, wherein the means for registering includes:
- a means for verifying and recording the identity of individuals registering;
 - a means for digitizing and recording handwritten signature of individuals registering;
 - a means for associating passwords with the recorded digitized handwritten signatures and the recorded identities; and
 - a means for storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being accessible to the local computer cluster.
42. (Amended 6/2/2004) The system of claim 41 further comprising:

a means for recording biometric measurements other than the handwritten signature of individuals registering;

a means for associating the biometric measurements of individuals registering with the recorded identities of the individuals registering; and

a means for storing the biometric measurements in the identity database.

43. (Original) The system of claim 42 further comprising a means of detecting using the biometric measurements whether individuals have previously registered.

44. (Original) The system of claim 36 wherein the first user is a registered user.

45. (Original) The system of claim 44 wherein the means of signing comprises:

a) a means of appending the first user's digitized signature to the signature ready document;

b) a means of making a hash of the signature ready document; and

c) a means of encrypting the hash of the signature ready document with the first user's complete private key.